Atty. Docket No. 080398.P481
Express Mail Label No. EL837201546

UNITED STATES PATENT APPLICATION

FOR

PROTECTING SECURED CODES AND CIRCUITS IN AN INTEGRATED CIRCUIT

INVENTOR:

Hidekazu Watanabe

PREPARED BY:

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(858) 457-0022

PROTECTING SECURED CODES AND CIRCUITS IN AN INTEGRATED CIRCUIT

BACKGROUND

[0001] The present invention relates to an integrated circuit, and more particularly, to protecting secured codes and circuits in such an integrated circuit.

[0002] It is often necessary in areas of electronic data processing to protect secret information or circuit from unauthorized access. However, in designing integrated circuits (IC), protection of these secret information or circuit may not be a priority task. This is because the information, the circuit, and the bus that carries the information are all internal to a chip or a board. Access to memories or other peripherals within the chip would normally go through a security apparatus in the chip/board.

[0003] If the IC includes a central processing unit (CPU), a digital signal processor (DSP), or other microprocessors, the IC may provide a debug function on these processors to develop software. Thus, the debug function provides access to the entire peripherals or memories. Accordingly, the debug function on the processor may provide unauthorized "back-door" access to the secret information or circuit.

SUMMARY

[0004] In one aspect, a security access system for an integrated circuit (IC) is disclosed. The system includes an access code generator and a security portal. The access code generator generates a key code that allows access to secured portions of the IC through a debug module in the IC. The security portal receives the key code from the access code generator, and allows access to the debug module if the key code matches a pre-stored code in the security portal.

[0005] In another aspect, an integrated circuit (IC) system is disclosed. The IC system includes a debugging tool, a processor, a plurality of peripheral device, a debug module, an access code generator, and a security portal. The peripheral devices may include secured portions, which may comprise secret codes or circuits. The debug module is coupled to the processor, and is arranged to receive commands from the debugging tool and to send data according to the commands. The access code generator generates a key code. The security portal is disposed between the debug module and the debugging tool. The security portal allows the commands from the debugging tool to pass to the debug module only when the key code from the access code generator matches an internally stored code in the security portal, such that the security portal operates to provide debugging tool with authorized access to the secured portions.

[0006] In a further aspect, a method for accessing secured portions of an integrated circuit (IC) through a debug module is disclosed. The method includes receiving a key code, determining if the received key code is correct, and enabling access to the debug module if a match is made.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] Figure 1 shows a typical layout of a conventional integrated circuit including at least a central processing unit (CPU) and a debug module.

[0008] Figure 2 is a more detailed diagram of a debug module and a debugger.

[0009] Figure 3 shows a security portal disposed between the debugger and the debug module in accordance with an embodiment of the present invention.

[0010] Figure 4 shows one implementation of the security portal design shown in Figure 3.

[0011] Figure 5 shows an alternative implementation of the security portal design shown in Figure 3.

[0012] Figure 6 illustrates a timing diagram of a security access process.

[0013] Figure 7 is a flowchart of the security access process according to an embodiment of the present invention.

DETAILED DESCRIPTION

[0014] In recognition of the above-stated problem with the prior design of the integrated circuit (IC), the present invention describes embodiments for providing a security portal for debugging tools to enable only authorized access to the debug module in the IC. Consequently for purposes of illustration and not for purposes of limitation, the exemplary embodiments of the invention are described in a manner consistent with such use, though clearly the invention is not so limited.

[0015] FIG. 1 shows a typical layout of a conventional integrated circuit 100 including at least a central processing unit (CPU) 104 and a debug module 102. In some cases, the debug module 102 may reside within the CPU 104. The circuit 100 may also include a program memory 106, which may include secret codes. The circuit 100 may further include a data memory 108, a secured peripheral device 110, and other peripherals 112. The devices and memories 104-112 may be connected through a bus 114. The debug module 102 provides the debugging tool 120 with access to the CPU 104 through a debug port 116 in the IC 100.

[0016] A more detailed diagram of the debug module 102 and the debugger 120 is shown in FIG. 2. The diagram also illustrates information exchange between the debug module 102 and the debugger 120 through the debug port 116. In the illustrated example, the debugger 120 sends a command to access memory or peripheral to the debug module 102, and the module 102 responds with data.

[0017] FIG. 3 shows a security portal 300 disposed between the debugger 302 and the debug module 304 in

accordance with an embodiment of the present invention. The security portal 300 is arranged in a configuration that allows access to the debug module 304 only when an access code 306 that matches the pre-stored code is received at the portal 300. Thus, this design prevents unauthorized access to the debug module 304, and subsequently, to the secret code or circuit in the peripheral devices.

[0018] One implementation of the security portal design 400 (described in conjunction with FIG. 3) is shown in FIG. 4. In the illustrated embodiment, the security portal 400 includes an AND gate 408 and a key matching circuit 410. Moreover, the access code circuit 306 (see FIG. 3) is implemented with a key generator circuit 406. In one embodiment, the key matching circuit 410 may be implemented with a comparator, while the key generator circuit 406 may be implemented with shift registers and/or counters.

[0019] When the debugger 402 sends a command to the debug module 404, the AND gate 408 in the security portal 400 intercepts the command and does not release the command until an enable signal is received from the key matching circuit 410. While the security portal 400 is in a reset mode, the enable signal stays de-asserted, at logic low level. This keeps the output of the AND gate 408 also de-asserted to prevent the debugger commands from reaching the debug module 404, and thus, prevent the debugger 402 from obtaining unauthorized access to the secret code or circuit. When the key generator 406 supplies a key that matches a pre-stored internal key in the key matching circuit 410, the key matching circuit 410 generates the enable signal. For example, if the pre-stored internal key code is set to '01011010', the key matching circuit 410 generates the enable signal only when the key generator 406 supplies the same serial code '01011010' to the key

matching circuit 410. This enables the debug command to reach the debug module 404, and hence, the secured portions of the IC.

[0020] An alternative embodiment of the security portal 500 is illustrated in FIG. 5. This embodiment provides an additional layer of security by adding a reset timer 508 to the design of FIG. 4. In the illustrated embodiment, the security portal 500 includes a first AND gate 502 and a key matching circuit 504 similar to those shown in FIG. 4. However, the security portal 500 of the present embodiment further includes a second AND gate 504 and a reset timer 508. The reset timer 508 sets a window of time period within which the matching key must be supplied by the key generator 510. Thus, the reset timer 508 provides a key unlock time window starting at a system reset point. In one embodiment, the reset timer 508 may be implemented with a flip-flop.

[0021] If a correct key code is supplied to the second AND gate 506 within the time window, an enable signal is then sent to the first AND gate 502 to enable the debug command. Otherwise, if a correct key code is not supplied within that time window, the reset timer 508 prevents the key matching circuit 504 from issuing an enable signal by triggering a key lock signal to the second AND gate 506. Therefore, even if a correct key code is supplied to the second AND gate 506, if the key code arrives after the time window set up by the reset timer 508, the debug command will not be enabled. Accordingly, this embodiment prevents unauthorized access to the secured portions of the IC chip by supplying a series of key code sequences until a key code matches the pre-stored key.

[0022] FIG. 6 illustrates the above-described process in a timing diagram. A reset signal 600 received by the reset timer 508 starts a key unlock time window 602 by triggering a key lock signal 604. If a correct key code 606 is received by the second AND gate 506 within the key unlock time window 602, an enable signal 608 is sent to the first AND gate 502. Moreover, the enable signal 608 enables the debug command to pass to the debug module 510. The length of the key unlock time window may be appropriately adjusted to allow sufficient time to enter the correct key code.

[0023] FIG. 7 is a flowchart of the security access process according to an embodiment of the present invention. The process enables only authorized access to the debug module. The process includes issuing a reset command to start a key unlock time window, at 700. If a correct key code is received (at 702), the security portal is unlocked, at 704, and the debug command is enabled, at 706. In an alternative embodiment, the correct key code must be received within the key unlock time window (at 702) to unlock the security portal and enable the debug command. Otherwise, if a correct key code is not received, the security portal is locked, at 708, and the debug command is disabled at 710.

[0024] There has been disclosed herein embodiments for providing a security portal for debugging tools to gain authorized access to the debug module in the IC. The access authorization is performed by the security portal by verifying that the correct key code is received within the key unlock time window.

[0025] While specific embodiments of the invention have been illustrated and described, such descriptions have been for purposes of illustration only and not by way of

limitation. Accordingly, throughout this detailed description, for the purposes of explanation, numerous specific details were set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the system and method may be practiced without some of these specific details. For example, the circuits in the security portal may be implemented with devices such as comparators, shift registers, counters, and/or flip-flops. In other instances, well-known structures and functions were not described in elaborate detail in order to avoid obscuring the subject matter of the present invention. Accordingly, the scope and spirit of the invention should be judged in terms of the claims which follow.